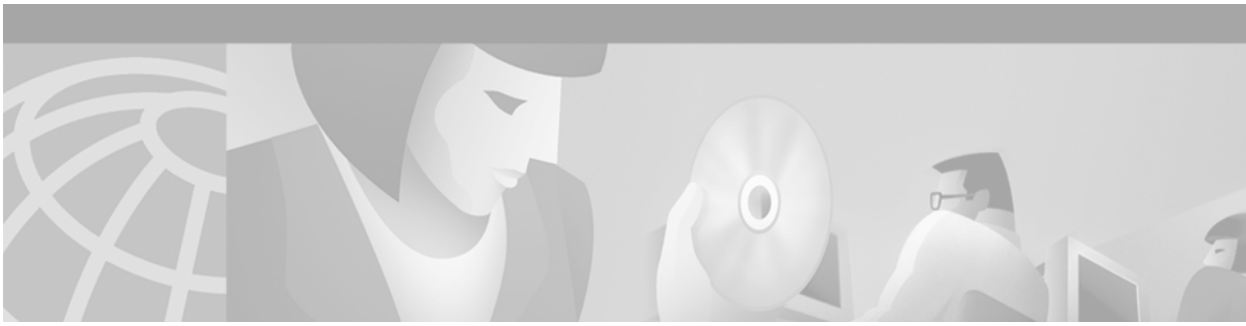

VPDN Group Session Limiting

Feature History

Release	Modification
12.2(1)DX	This feature was introduced.
12.2(2)DD	This feature was integrated into Cisco IOS Release 12.2(2)DD.

This document describes the VPDN Group Session Limiting feature in Cisco IOS Release 12.2(2)DD. It includes the following sections:

Feature Overview

Before the introduction of the Virtual Private Dial Network (VPDN) Group Session Limiting feature, you could only globally limit the number of VPDN sessions on a router with limits applied equally to all VPDN groups. Using the VPDN Group Session Limiting feature, you can limit the number of VPDN sessions allowed per VPDN group. This feature is implemented with the introduction of the **session-limit** *number* command in VPDN configuration mode. VPDN group session limiting is applied after the global VPDN session limiting (which is configured via the **vpdn session-limit** *session* command in configuration mode) is enforced.

Benefits

The VPDN Group Session Limiting feature gives more control to network administrators by enabling them to limit how many sessions a VPDN group can terminate. This feature enables service providers to cater to all types of organizations, large or small, by enabling finer configuration granularity.

Restrictions

- VPDN group session limiting cannot be configured on an L2TP Access Concentrator (LAC) or L2F Network Access Server (NAS).
- The range of legal values for *number* is from 0 to 32767.
- VPDN group session limiting applies only to L2F and L2TP sessions.

Related Features and Technologies

- Shell-Based Authentication of VPDN Users
- Accounting of VPDN Disconnect Cause
- Resource Pool Management

Related Documents

- *Resource Pool Management*
- *Shell-Based Authentication of VPDN Users*
- "Configuring Virtual Private Networks" section of the *Cisco IOS Dial Services Configuration Guide: Network Services*
- *Cisco IOS Dial Services Command Reference*

Supported Platforms

- Cisco 7200 series
- Cisco 7401 ASR router

Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at http://www.cisco.com/register.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. As of May 2001, Feature Navigator supports M, T, E, S, and ST releases. You can access Feature Navigator at the following URL:

http://www.cisco.com/go/fn

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

A VPDN session group must be created before the session-limit VPDN configuration group can be configured. You must configure the **accept-dialin** command or **request-dialout** command before VPDN session group limiting can be configured.

Configuration Tasks

See the following section for the configuration task necessary to configure the VPDN Group Session Limiting feature:

- Configuring VPDN Group Session Limiting, page 3 (required)

Configuring VPDN Group Session Limiting

To configure VPDN group session limiting, follow the steps in the table below, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn-group name`	Select the VPDN group to configure. *name*—Name of the VPDN group.

Step 2	`Router(config-vpdn)# accept-dialin`
	or
	`Router(config-vpdn)# request-dialout`
		Enables the router to accept dial-in requests.
		
		Enables the router to send L2TP dial-out requests.

Step 3	`Router(config-vpdn-acc-in)# protocol [l2f | l2tp]`	Specifies which tunneling protocol is to be used.

	Command	Purpose
Step 4	`Router(config-vpdn-acc-in)# virtual-template template-number`	Specifies the number of the virtual template that will be used to clone the virtual access interface. • *template-number*—Number of the virtual template that will be used to clone virtual-access interfaces. Valid range is 1 to 200.
Step 5	`Router(config-vpdn-acc-in)# exit`	Exits VPDN accept-dialin interface mode.
Step 6	`Router(config-vpdn)# terminate-from hostname host-name`	Accepts tunnels that have this host name configured as a local name. • *host-name*—The host name that this VPDN group will accept connections from.
Step 7	`Router(config-vpdn)# session-limit session-number`	Limits the number of sessions allowed on the specified VPDN group. • *session-number*—The maximum number of sessions allowed on the specified VPDN group in the range of 0 to 32767. If **session-limit** is configured to 0, no sessions are allowed on the VPDN group.

Verifying VPDN Group Session Limiting

Follow the steps below to verify the successful configuration of VPDN group session limiting:

Step 1 Enter the **session-limit 1** command in VPDN configuration mode.

Step 2 Establish a VPDN session by dialing in to the network access server (NAS) using an allowed username and password.

Step 3 Attempt to establish another VPDN session by dialing in to the NAS using another allowed username and password.

Step 4 A Syslog message similar to the following should appear on the console of the router:

```
00:11:17: %VPDN-6-MAZ_sESS_EXCD:L2F HGW great_went has exceeded configured local
session-limit and rejected user user@anywhere.com
```

Step 5 Enter the **show vpdn history failure** command on the router. If you see output similar to the following, the group session limit was successful:

```
User: user@anywhere.com
NAS: clifford_ball, IP address = 172.25.52.8, CLID = 2
Gateway: great_went, IP address = 172.25.52.7, CLID = 13
Log time: 00:04:21, Error repeat count:1
Failure type: Exceeded configured VPDN mazimum session limit
Failure reason:
```

Monitoring and Maintaining VPDN Group Session Limiting

Use the following commands to monitor and maintain VPDN group session limiting:

Command	Purpose
`Router# show vpdn group name`	Displays the session-limit set, and the number of active sessions and tunnels on the specified VPDN group. • *name*—VPDN group name summarizes the configuration of the specified group.
`Router# show vpdn`	Displays a summary of all active VPDN tunnels.
`Router# show vpdn history failure`	Displays information about VPDN user failures.
`Router# show vpdn session [all [interface | tunnel | username] | packets | sequence | state | timers | window]`	Displays VPDN session information including interface, tunnel, username, packets, status, and window statistics. • **all**—All session information for active sessions. – **interface**—Interface associated to a specific session. – **tunnel**—Tunnel attribute filter. – **username**—Username filter. • **packets**—Packet/byte count. • **sequence** —Sequence numbers. • **state**—State of each session. • **timers**—Timer information. • **window**—Window information.
`Router# show vpdn tunnel [all [id | local-name | remote-name] | packets | state | summary | transport]`	Displays VPDN tunnel information including tunnel protocol, ID, local and remote tunnel names, packets sent and received, tunnel, and transport status. • **all**—All information for active tunnels. Options are: – **id**—Local tunnel ID. – **local-name**—Name of local end of tunnel. – **remote-name**—Name of remote end of tunnel. • **packets**—Packet/byte count. • **state**—Tunnel state information. • **summary**—Tunnel information summary. • **transport**—Tunnel transport information.

Configuration Examples

This section provides the following configuration examples:

Configuring VPDN Group Session Limiting

In the example below, VPDN group “abc” is created and restricted to three sessions:

```
Router# configure terminal
Router(config)# vpdn-group abc
Router(config-vpdn)# accept dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# terminate hostname host1
Router(config-vpdn)# session-limit 3
Router(config-vpdn)# end
Router# show vpdn-group abc
```

Command Reference

This section documents the modified command that configures the VPDN Group Session Limiting feature. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **session-limit (vpdn)**

session-limit (vpdn)

To limit the number of sessions that are allowed through a specified VPDN group, use the **session-limit** command in VPDN configuration mode. To remove a configured session-limit restriction, use the **no** form of this command.

session-limit *number*

no session-limit *number*

Syntax Description

number	Specifies the number of sessions allowed through a specified VPDN group.

Defaults

No default behavior or values.

Command Modes

VPDN configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.

Usage Guidelines

Use this command to limit the number of allowed sessions for a specified VPDN group.

This command works independently from the global VPDN **session-limit** command. Using the global VPDN **session-limit** command, you can restrict the total number of sessions allowed on all VPDN groups. Global session limiting is configured in configuration mode. VPDN group session limiting is configured in VPDN configuration mode.

Global VPDN session limiting and per VPDN group session limiting work independently, but global VPDN session limiting is enforced before individual VPDN group limiting. For example, if you configure **vpdn session-limit 2** at the global configuration mode and **session-limit 3** under the VPDN group "abc," no more than two calls are allowed in VPDN group "abc."

Examples

The following example creates VPDN group "abc," virtual template 5, and restricts VPDN group "abc" to three sessions:

```
Router(config)# vpdn-group abc
Router(config-vpdn)# accept dialin
Router(config-vpdn-acc-in)# protocol l2tp
Router(config-vpdn-acc-in)# virtual-template 5
Router(config-vpdn-acc-in)# exit
Router(config-vpdn)# terminate hostname host1
Router(config-vpdn)# session-limit 3
```

Related Commands

Command	Description
session-limit	Limits the number of VPDN sessions.